EXHIBIT B

GRAF & PITKOWITZ
RECHTSANWÄLTE GMBH

www.gpp.at

Stadiongasse 2
A-1010 Vienna
Tel +43 (1) 401 17-0
Fax +43 (1) 401 17-40

Marburger Kai 47
A-8010 Graz
Tel +43 (316) 833 777-0
Fax +43 (316) 833 777-33

Court of Registration
Commercial Court Vienna
FN 255087 d
DVR 0993433
UID ATU 61238734

Vienna Office
Dr. Ferdinand Graf
graf@gpp.at

DRAFT!
Via E-mail

Mr. Michael Leidig
CENTRAL EUROPEAN NEWS LIMITED
Vienna branch office
Hadikgasse 96
1140 Wien
editor@cen.at

22 December, 2016

W:\33\Graffe\033\DRAFT Memo For Mr Leidig 22.12.2016.Docx

Restrictions under Austrian Law for Transmitting Personal Data to U.S. Authorities

Dear Mr. Leidig,

During our telephone conversation on 20 December 2016, you asked me to provide you with a legal analysis on the restrictions under Austrian data protection law for data transfers to U.S. authorities.

1. Summary

1.1. Under Austrian law, you cannot be forced to disclose the Data if it was obtained by a journalist for your journalistic profession.

1.2. A transfer of Data to U.S. authorities would require

- a positive admissibility check (point 3.2.2)
- a "prior checking" by the Austrian data protection authority (in case of crime-related or sensitive data, point 3.2.3)
- a transfer permit of the Austrian data protection authority (point 3.2.3)

in order to be in compliance with Austrian data protection law. If even one requirement is not met, you are not allowed to transfer the Data, otherwise risking legal consequences (point 3.2.4).

2. Facts of the case / Presumptions

From our conversation, I understand that these are the facts of the case:

- You are a journalist that operates a media company with a branch office in Vienna.
- Certain data has been provided to you ("**Data**").
- This Data was collected and is stored in Austria.
- U.S. authorities requested the discovery of the Data.

This analysis is further based on the following presumptions:

- The Data contains personal data; i.e. information relating to data subjects who are identified or identifiable (section 4 (1) of the Austrian Data Protection Act ("**DSG**")).
- The Data may also contain sensitive data; which is a special category of personal data relating to natural persons concerning their racial or ethnic origin, political opinion, trade-union membership, religious or philosophical beliefs, and health or sex life (section 4 (2) DSG).
- The Data may also contain crime-related data, which is a special category of personal data concerning acts and omissions punishable by the courts or administrative authorities (section 8 (4) DSG).

3. Legal Analysis

3.1. Protection of Editorial Confidentiality (Section 31 of the Austrian Media Act)

Pursuant to Section 31 of the Austrian Media Act, media owners, editors, copy editors and employees of media undertaking or media service, as witnesses in criminal proceedings or other proceedings before a court or an administrative authority, have the right to refuse answering questions concerning the person of an author, sender or source of articles and documentation or any information obtained for their profession.

This right of protection of editorial confidentiality is very broad and must not be by-passed by requesting the person enjoying this right to surrender documents, printed matter, image, sound or data carriers, illustrations or other representations of such contents or confiscating them.

Thus, pursuant to Austrian law, you cannot be forced to disclose the Data if it was obtained for your journalistic profession.

3.2. Data Protection Law

3.2.1. Territorial Scope

Based on the facts and presumptions outlined in point 2 above, Austrian data protection law is applicable to the case on hand. The Data was collected and is stored in Austria and you have a branch office in Austria to which the Data can be ascribed.

3.2.2. Admissibility check

Under Austrian law every form of use of personal data is prohibited unless an exemption to this prohibition applies. There are certain exceptions for the use of data for journalistic purposes; however, we understand that the disclosure in question is not one for journalistic purposes thus the DSG will apply.

Pursuant to section 7 DSG, a data transfer is only permissible if:

- The data originates from a "legal data application" (i.e. data that was processed only insofar as the purpose and content of the data application are covered by the statutory competencies or the legitimate authority of the respective controller and the data subjects' interest in secrecy deserving protection was not infringed), and
- the recipient has satisfactorily demonstrated to the transmitting party his statutory competence or legitimate authority with regard to the purpose of the transmission, insofar as it is not beyond doubt, and
- **the data subject's protection-worthy interests in secrecy are not infringed by the purpose and content of the transmission.**

The data subject's protection-worthy interests in secrecy with regard to **"regular" personal data** (i.e. no sensitive or crime-related data) are **not infringed if** (section 8 DSG):

- an explicit legal authorization or obligation to use the data exists; or
- the data subject has given his consent (can be revoked at any time!); or
- vital interests of the data subject require the use; or
- over-riding legitimate interests pursued by the controller or by a third party require the use of data (balancing of interests).

In case of **crime-related data**, the data subject's protection-worthy interests in secrecy **are not infringed if** (section 8 (4) DSG):

- an explicit legal obligation or authorization to use the data exists; or
- the legitimacy of the data application otherwise follows from statutory responsibilities or other legitimate interests of the controller that override the data subjects' interests

in secrecy deserving protection and the manner of use safeguards the interests of the data subject according to this federal law or

- the transmitting of data is made for a report to an institution in charge of prosecution of a reported criminal act.

In case of **sensitive data**, the possibilities of use are even more restricted. Sensitive data **may be used** (i.e. the use does not infringe the data subject's protection-worthy interests in secrecy) **only if one of the very restrictive exemptions contained in section 9 DSG applies.** With regard to sensitive data, there is no balancing of interests – irrespective of whether there are over-riding legitimate interests for the use of the sensitive data, it cannot be used if none of the section 9 DSG exemptions applies. Some of the section 9 DSG exemptions are:

- the data are used only in indirectly personal form (i.e. the identity of the data subject cannot be established by legal means).
- the obligation or authorization to use the data is stipulated by laws, insofar as these serve an important public interest, or
- the data subject has unambiguously given his consent, which can be revoked at any time, the revocation making any further use of the data illegal, or
- the use is necessary for establishment, exercise or defence of legal claims of the controller before a public authority and the data were collected legitimately.

If even one of the above-mentioned requirements (section 7, 8, 9 DSG) is not fulfilled, the Data may not be transferred!

3.2.3. Further requirements

In case of crime-related and sensitive data, a **"prior checking" by the Austrian Data protection authority** is required (the Austrian protection authority checks whether or not crime-related and sensitive data can be used).

A transfer to U.S. authorities also requires a **transfer permit of the Austrian data protection authority**: From an Austrian perspective, the U.S. is not considered as a "country with an adequate level of data protection" (sections 12 and 13 DSG). As a consequence, a data controller must apply for a **transfer permit** with the Austrian data protection authority for every data transfer to a recipient in the U.S. (that is not certified under the EU – U.S. Privacy Shield). Such permit is only granted if it can be proven that, despite the recipient being in a country with no adequate level of data protection

- an adequate level of data protection is given in this specific case or

- the controller can satisfactorily demonstrate that the interests in secrecy deserving protection of the data subject of the planned data exchange will be respected outside of Austria.

Considering that the predecessor of the EU – U.S. Privacy Shield (i.e. the Safe Harbor regime) was declared invalid by the European Court of Justice after the revelations of Edward Snowden – among others because of the insufficient protection of the data transferred to the U.S. against surveillance by the U.S. public authorities – it **not very likely** that the Austrian data protection authority, who happens to be very strict, **will permit the transfer** of the Data to the U.S. authorities.

3.2.4. Consequences in case of an infringement of Austrian data protection law

There are multiple consequences to be borne by you in case of an infringement of Austrian data protection law. Not only do most infringements constitute administrative offences that are subject to high administrative fines, you can also be found liable for the damages suffered by the data subject whose interests in secrecy have been infringed.

If the Data is subject to contractual confidentiality obligations (i.e. you have undertaken not to disclose the Data), a breach may also make you liable for damages resulting from a breach of this contractual obligation.

Should you have any further queries, please feel free to contact us.

With best regards,

Graf & Pitkowitz Rechtsanwälte GmbH
Ferdinand Graf